Report on "Distribution Internet-Based Load Altering Attacks against Smart Power Grids"

***Abstract*— Utilities all over the world consider the wide spread integration of communication technology in modern power networks. The main obstacle that faces these kind of technologies is the existing of new strategies for cyber intrusion in the direct load control command signals and demand side management price signals to cause grid instability or blackout through locations vulnerable to the Internet attacks. This report discusses that paper that focus on cyber-attacks against the consumption sector only through explaining the target loads and the defense mechanisms block these types of attacks. The simulation results proposed cost efficient load protection plan to optimize the cost of protection and ensure that the unprotected loads can't cause overflow to the circuit or any other harms to the smart grid security.**

***Index Terms*— Demand side management, Internet based load altering attacks, Cost efficient load protection, smart grid security.**

I. Introduction

THE RECENT revolution in power system smart grids, at all sectors: generation, distribution and control, and consumption, can significantly utilize the modern communication and computation technologies, such as two way communication capability through smart meters, for delivering reliable and secured energy, as well as improving the efficiency of stability operation for the whole entire power grid [1].

Covering security for every sector in the power system needs unfathomable requirements and if done incorrectly, can open new vulnerabilities in the infrastructure of the grid to Internet based load altering attacks [2].

There are three different scenarios of cyber-attacks according to the target sector of the attacks as shown in Fig. 1. Type I cyber-attacks target the generation sector. Despite these type of attacks require advanced resources in order to be completed, they have been succeeded in January 2008 for four cities [3].

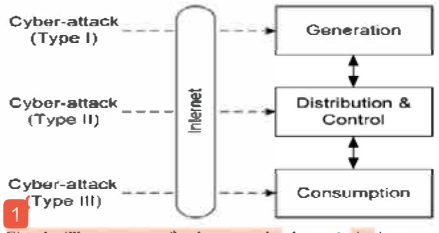

Fig. 1. Three types of cyber-attacks through the internet.

M.W.Abdelghany is PhD student with the Electrical and computer Engineering Department, Concordia University, Montreal, Quebec, Canada. (E-mail: m_eldes@encs.concordia.ca)

More information about the defense mechanisms for this category can be found in [4].

Type II cyber-attacks target the distribution and control and dispatching centers sector. The hackers attempt to inject false data or errors in the state variables collected from the measurement sensors toward the supervisory control and data acquisition (SCADA) to cause grid instability; blackout or damage to the grid equipment [4], [5].

Type III cyber-attacks target the consumption sector; which the report on this paper is focus on. Attackers exploit the increase in usage of demand side management (DSM) techniques, using the internet and distributed software, to attack the most critical locations for causing overflow in the circuit or disaster to the power transmission and user equipment. The contribution for this report can be concluded as follows.

- An overview about the different types of target loads that could be vulnerable to attackers to utilize them to cause major disaster to the grid.
- An identification for multiple scenarios of defense mechanisms against this kind of cyber-attacks and how to secure the price and command signals.
- A proposal strategy for cost efficient load protection that secure only the key locations in the grid only and at the same time ensure that the safety of the grid is not risky.

The rest for this report is summarized as follows. In Section II, it illustrates how the internet based load altering attacks can take place against three different type of target loads. While in Section III, it shows a package of defense mechanisms that can be used to block this type of cyber-attacks. An optimization technique apply cost efficient load protection case study is discussed in Section IV. Conclusion and future work are explained in Section V.

II. Target Loads Through the Internet

Internet based load altering attacks target a huge number of loads and consumption units that use the internet at the utmost vulnerable areas in the electric network to disperse the balance between the supply and demand profiles. Next, there is explanation for three types of loads that use internet.

A. Data Centers and Computation Load

Data center's energy consumption is very huge as it contains computer servers with hundreds of thousands and substation transformers like what owned to Google and Microsoft. So, attackers utilize them to cause load fluctuations and as a result a massive effect on the electric network [6].

B. Direct Load Control

Applying demand side management programs, such as the direct load control, to improve system operation through minimizing peak time load and maximizing load factor. These programs use internet to send command signals include on/off switches. Attackers can make huge spike through sending fabricated commands to the residential and industrial loads which results problems in power quality and voltage [7].

C. Indirect Load Control

End users are allowed through smart meters to control their loads independently using the price signals that are send by the utility via the internet to minimize the energy consumption bill through shifting loads from peak to off peak hours. So, attackers fabricate signals to inject false prices to cause changes in thousands of residential load profiles and as a result grid instability [8].

III. Defense Mechanisms and Challenges

As discussed in section I, the attacks takes place in a different categories. So, in this section a package of defense mechanisms will be implemented to block the Internet based load altering attacks.

A. Protecting Command and Price Signals

Usually command signal messages transmissions are unicast that exclusive to particular user (Direct load control), while price messages transmissions are multi cast that announced to all users (Indirect load control). Upon this, to protect these signals, it is recommended to utilize private key encryption and message authentication code (MAC) and group key management respectively as shown in Fig. 2 [8],[9].

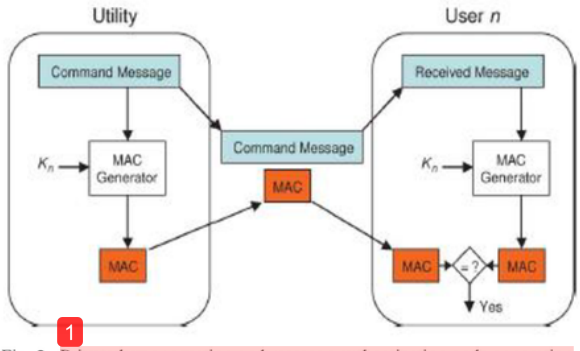

Fig. 2. Private key encryption and message authentication code generation.

B. Protecting Smart Meters and Data Centers

The smart meters protection sectors scheme are confidentiality, integrity, availability and accountability that could be settled up through using passwords, firewalls and identity authentication. As well as data centers the must be protected against denial of service and computation attacks [10].

C. Attack Detection and Learning Demand Patterns

This mechanism requires to learn the load pattern for the residential and commercial demands at each region to observe the abnormal changes [9].

D. Load Shedding and Load Relocating

This mechanism used to shut down the loads at locations (load shedding) where the attacks are detected with high probability, then move certain type of loads from one place to another (load relocating) to keep more balanced load distribution [11].

IV. Cost Efficient Load Protection Case Study

A proposed scheme to implement partial load protection at the most critical locations instead of full load protection to minimize the cost.

A. Mathematical Formulation

Let N a set of all buses in a network. Total active load power at bus i is: $P_i = L_i + (1 - \alpha_i)\Delta_i - G_i$ (1)

G_i represents active power generated at bus i. L_i represents active load power at bus i. Δ_i represents maximum extra active load power that can be added to bus i. α_i denotes portion of extra load at bus i which is protected. DC power flow equations are [12]:

$$G_i - L_i - (1 - \alpha_i)\Delta_i = \sum_{j=1, j\neq i} B_{ij}\left(\theta_i - \theta_j\right) \; \forall\, i \in N \quad (2)$$

$$P_{ij} = B_{ij}\left(\theta_i - \theta_j\right) \forall\, i, j \in N \quad (3)$$

$$P_{ij} < P_{ij}^{max} \; \forall\, i, j \in N \quad (4)$$

Where, B_{ij} represents the imaginary term in the complex value at row i and column j of Y-bus matrix of the grid. P_{ij} denotes the power flow over each branch (i, j). P_{ij}^{max} denotes the power transmission capacity of branch (i, j). θ_i denotes the voltage phase angle at bus i. Let $C_i(\alpha_i)$ the cost of load protection. So, it is required to get the cost efficient load protection from optimizing the following problem:

$$\underset{\alpha}{minmize} \; \sum_{i\in N} C_i(\alpha_i) \text{ Subject to Equations [(2) – (4)]} \quad (5)$$

By solving (5), the cost is optimized and the amount of load protection at each bus is determined and leads to family of linear functions as shown in Fig. 3, where

$$0 < \alpha_i^{C(1)} < \alpha_i^{C(2)} < \cdots < \alpha_i^{C(K_i-1)} < 1 \quad (6)$$

K_i represents the number of load classes at bus i needed to be protected. $\alpha_i = 0$ if no load is being protected at bus i. From zero to $\alpha_i^{C(1)}$ the loads are in the class with the lowest cost of protection. The further increasing α_i, the highest cost of protection required, until it reaches the full load protection, if needed and $\alpha_i = 1$.

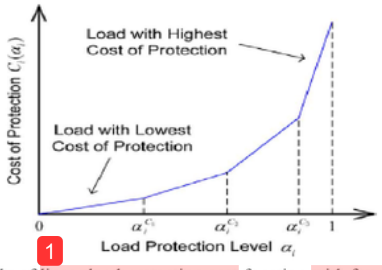

Fig. 3. Family of linear load protection cost function with four load classes.

B. Case Study

A power grid consists of 24 buses and 38 branches with nine buses fixed generation capacity and a reserve generator at bus 22 to balance supply and demand as shown in Fig. 4. This is an edited version of the IEEE 24-bus reliability test system [13].

The system consists of 10 buses where the demands don't utilize the internet; so, there is no risk to be vulnerable to the internet based load altering attacks. While there are other 8 buses that are accessible through the internet. Moreover, there are units at buses 7 and 20 assumed to be direct load control, indirect load control at buses 3 and 23 and demand side management units at buses 3,7,20 23. It is assumed that $K_i = 2$, $\alpha_i^1 = 0.5$ for $i \in \{1, 3,7,13,15,18,20,23\}$ and $P_{ij}^{max} = 400\ MW$.

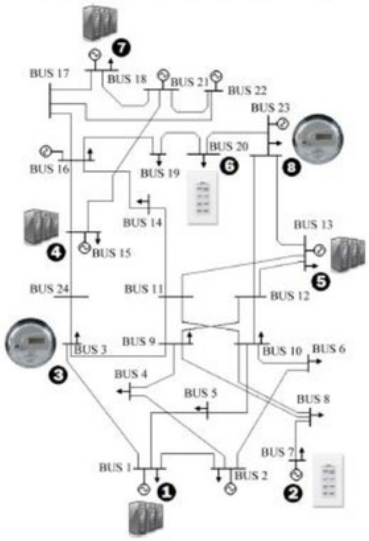

Fig. 4. IEEE 24-bus reliability test system.

C. *Simulation Results*

Three load protection scenarios are implemented on the power grid in Fig. 4. By applying no load protection scenario, there will be an over power flow (440 MW) on one transmission line only which is branch (16, 17).While implementing full load protection scenario, there will be no over power flow on any of the eight buses that using the internet. Using the optimal cost efficient load protection scenario, the cost is 10.2% from total cost in full load protection and only it is required to protect half of the direct load control at bus 20 ($\alpha_{20} = 0.5$), quarter of the indirect load control at bus 23 ($\alpha_{23} = 0.22$) and half of computation load at bus 13 ($\alpha_{13} = 0.5$). In addition, $\alpha_i = 0$ for all $i \in N \backslash \{3,20,23\}$. As a result, the grid parameters has an effect on the cost of efficient load protection. As capacity of transmission lines increases, the cost of efficient load protection drops with respect to the full load protection as in Fig. 5.

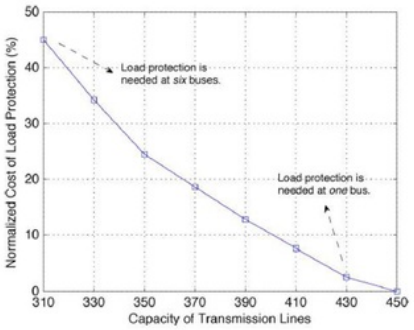

Fig. 5. Optimal cost efficient load protection for different line capacities.

On the other hand, the optimal cost of efficient load protection depends on the place of the spinning reserve generator as the cost could be as low as zero if this generator exist at one of the buses (1, 2,…, 6) or it could be as high as 16% if the spinning reserve generator places at bus 13 as shown in Fig. 6. So, it is necessary to take grid topology and parameters into consideration.

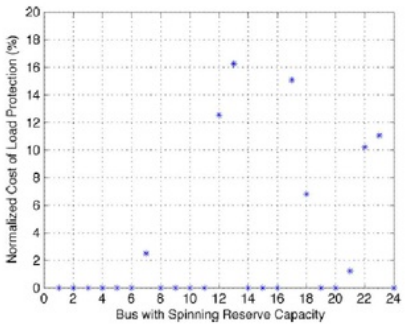

Fig. 6. Bus with Spinning Reserve Capacity.

V. CONCLUSION AND FUTURE WORK

This report has been showed a full summary for the paper to understand the Internet based load altering attacks in the power smart networks. Three types of vulnerable load classes that access through the internet have been discussed and how a defense mechanisms could block that attacks. To sum up, this paper proposed a strategy to optimize the cost of load protection and prevent the grid from overloading or any other harms.

REFERENCES

[1] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proc. IEEE*, vol. 105, no. 5, pp. 1058–1070, May 2016.

[2] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[3] S. M. Amin, "Securing the electricity grid," *Bridge*, vol. 40, no. 1, pp. 13–20, Mar. 2010.

[4] W. F. Boyer and S. A. McBride, "Study of security attributes of smart grid systems current cyber security issues," Idaho Natl. Lab. Tech. Rep., Apr. 2009.

[5] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, Oct. 2010.

[6] A. H. Mohsenian-Rad and A. Leon-Garcia, "Energy-information transmission tradeoff in green cloud computing," in *Proc. IEEE Globecom'10*, Miami, FL, Dec. 2010.

[7] N. Ruiz, I. Cobelo, and J. Oyarzabal, "A direct load control model for virtual power plant management," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 959–966, May 2009.

[8] A. H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 320–331, 2010.

[9] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Comput. Surveys*, vol. 35, no. 3, pp. 309–329, 2003.

[10] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Pittsburgh, PA, Jul. 2008.

[11] A. H. Mohsenian-Rad and A. Leon-Garcia, "Coordination of cloud computing and smart power grids," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, Oct. 2010.

[12] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*. New York: Wiley-Interscience, 1996.

[13] Reliability Test System Task Force, Application of Probability Methods Subcommittee, "The IEEE Reliability Test System—1996," pp. 1010–1020, Aug. 1999.

Student.pdf

ORIGINALITY REPORT

23%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.ee.ucr.edu Internet	228 words — 12%
2	Mohsenian-Rad, Amir-Hamed, and Alberto Leon-Garcia. "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids", IEEE Transactions on Smart Grid, 2011. Crossref	125 words — 6%
3	www.myweb.ttu.edu Internet	42 words — 2%
4	Suleiman, Husam, Israa Alqassem, Ali Diabat, Edin Arnautovic, and Davor Svetinovic. "Integrated smart grid systems security threat model", Information Systems, 2015. Crossref	17 words — 1%
5	www.cyberjournals.com Internet	14 words — 1%
6	www.apsipa.org Internet	10 words — 1%
7	Sicilia F. Judice, Bruno Barcellos S. Coutinho, Gilson A. Giraldi. "Lattice methods for fluid animation in games", Computers in Entertainment, 2009 Crossref	8 words — < 1%

EXCLUDE QUOTES ON
EXCLUDE BIBLIOGRAPHY ON
EXCLUDE MATCHES OFF